What is claimed is:

1. A system for verifying a digital signature, comprising:

a first computer having a certificate and a signed message;

a second computer configured to receive the certificate and the signed message; and

a third computer configured to receive the certificate and the signed message from the second computer for a validation request, to validate the certificate and to generate a certificate validation statement in response thereto, and to provide an acknowledgement and a public key to the second computer, the acknowledgement comprising in part the certificate validation statement, the signed message, a first proof portion having a confirmation associated with the certificate validation statement and the signed message in combination, and a second proof portion having a signed digest having the confirmation as part of a set of confirmations.

2. The system of claim 1 further comprising a fourth computer configured to receive the certificate, the signed message, the acknowledgement and the public key.

3. The system of claim 2 further comprising a certificate authority configured to provided the certificate to the first computer.

4. The system of claim 3 wherein the certificate authority is configured to provide validation information to the third computer.

5. A system for verifying a digital signature, comprising:

a plurality of first computers each having a certificate of a set of certificates and a respective signed message signed in association with the certificate;

a plurality of second computers in communication with the first computers and configured to receive respective certificates and associated signed messages; and

a third computer in communication with the second computers and configured to receive validation requests for the certificates and the signed messages from the plurality of second computers, the third computer configured to validate the certificates, to generate a certificate validation statements, and to provide each of the second computers an acknowledgement and a public key, the acknowledgement comprising in part a certificate validation statement, the signed message, a first proof portion having a confirmation associated with the certificate validation statement and the signed message in combination, and a second proof portion having a signed digest having the confirmation as part of a set of confirmations for the second computers.

6. The system of claim 5 further comprising a fourth computer in communication with the third computer and configured to confirm at least a portion of the acknowledgement.

7. A method for validating a signature of a signed message corresponding to a certificate, comprising;

providing validation information to a notary;

validating the certificate to create a certificate validation;

generating a confirmation in response to the certificate validation;

maintaining a set of confirmations where the confirmation is an element of the set;

generating a digest for the set of confirmations; and

signing the digest with a private key to create a signed digest.

8. The method of claim 7 further comprising:

providing the signed digest, the certificate validation, the confirmation, the signed message and the set of confirmations in response to receiving the certificate and the signed message.

9. The method of claim 8 further comprising providing a public key corresponding to the private key.

10. The method of claim 7 further comprising:

signing the confirmation, the set of confirmations and the signed digest configured to provide a digital signature with a hash chain.

11. A process for verifying a digital signature of an associated dated certificate in a system having a certificate authority, a notary and a time stamping authority, the certificate authority providing the notary with information on a plurality of dated certificates, the process comprising:

receiving a time-stamped signed message and a portion of the dated certificate;

using the portion of the dated certificate to locate the dated certificate from among the plurality of dated certificates;

validating the dated certificate as to time, date and non-revoked status;

providing a validation dated certificate and the time-stamped signed message as a status; and

signing the status with a private key.

12. The method of claim 11 further comprising sending a public key, the status and the status signed with the private key to an entity requesting validation.

13. A signal-bearing medium containing a program which, when executed by a processor in response to receiving a certificate, a signed message corresponding to the certificate and a request for validation, causes execution of a method comprising:

validating the certificate to create a certificate validation;

generating a confirmation in response to the certificate validation;

maintaining a set of confirmations where the confirmation is an element of the set;

generating a digest for the set of confirmations; and signing the digest with a private key to create a signed digest.

14. A process for verifying a digital signature of an associated dated certificate in a system having a certificate authority and a notary, the certificate

authority providing the notary with information on a plurality of dated certificates, the process comprising:

providing a signed first status, the signed first status including a message and the dated certificate;

providing at least a portion of the dated certificate;

using the portion of the dated certificate to locate the dated certificate from among the plurality of dated certificates;

validating the dated certificate as to date and non-revoked status;

providing a validation dated certificate and the signed first status as an unsigned status;

adding the unsigned status into a set of statuses for the date; and

signing the unsigned status with a private key to provide a signed second status.

15. The process of claim 14 further comprising:

generating a digest of the set of statuses;

providing the digest to a third party for dating and signing.

16. The process of claim 15 wherein the third party is a certificate authority.